INFORMATION AND CONTROL **48**, 70–79 (1981)

A Construction of Nonlinear Codes Which Betters or Equals Known Results for Certain Parameters

JAMES A. WISEMAN

Department of Mathematics, Boston University, Boston, Massachusetts 02215

A new technique for constructing non-linear codes is presented, which, in at least two cases, yields larger codes of a given length and minimum distance than any previously known code (according to the table in F. J. MacWilliams and N. J. A. Sloane's "The Theory of Error Correcting Codes", North-Holland, Amsterdam, 1977). The technique depends largely on identifying elements of $GF(2^k)$ with rows of a particular class of binary matrices. Several examples of the general theorem are given.

The objective of this paper is to present a method of constructing non-linear codes which will, in at least two cases, generate more code words for a fixed length and a fixed minimum distance than any known[1] code. The construction will also equal the best known results in several other instances (sometimes by making use of slight variations on the original idea). The construction will rely heavily on certain properties of Hadamard matrices. It will also make use of the following proposition.

LEMMA. *Let V be a vector space of dimension n over the field $GF(q)$ where $1 < n \leqslant q$. Then $\exists q$ sets of vectors in V, each set containing q vectors, so that the Hamming distance between any two vectors in the same set $=n$, while the Hamming distance between two vectors in different sets $\geqslant n-1$.*

Proof. Assume vectors in V are represented in standard form and note that it suffices to prove the lemma for $n = q$, since then deleting $q - n$ coordinates would give the general case. Now consider the following q matrices, each matrix having dimension $q \times q$:

$$X, A, \alpha A, \alpha^2 A, \ldots, \alpha^{q-2} A,$$

where

[1] According to Appendix A of MacWilliams and Sloane (1977).

0019-9958/81/010070-10$02.00/0

(i) α is a primitive element in $GF(q)$,

(ii)
$$X = \begin{bmatrix} \overbrace{0 \quad 0 \quad 0 \cdots 0 \quad 0}^{q \text{ times}} \\ 1 \quad 1 \quad 1 \cdots 1 \quad 1 \\ \alpha \quad \alpha \quad \alpha \cdots \alpha \quad \alpha \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \alpha^{q-2} \quad \alpha^{q-2} \quad \alpha^{q-2} \quad \alpha^{q-2} \quad \alpha^{q-2} \end{bmatrix} q,$$

(iii) A is the addition table for $GF(q)$, i.e.,

$$A = \begin{array}{c} \\ 0 \\ 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{q-2} \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \end{array} \\ \begin{bmatrix} 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & 1+1 & 1+\alpha & 1+\alpha^2 & \cdots & \alpha^{q-2} \\ \alpha & (\alpha+1) & (\alpha+\alpha) & (\alpha+\alpha^2) & \cdots & \alpha+\alpha^{q-2} \\ \alpha^2 & (\alpha^2+1) & (\alpha^2+\alpha) & (\alpha^2+\alpha^2) & \cdots & \alpha^2+\alpha^{q-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{q-2} & (\alpha^{q-2}+1) & (\alpha^{q-2}+\alpha) & (\alpha^{q-2}+\alpha^2) & \cdots & \alpha^{q-2}+\alpha^{q-2} \end{bmatrix} \end{array}.$$

(A is the matrix inside the brackets.) Then the rows of these matrices, considered as vectors in V and grouped according to which matrix they belong to, satisfy the statement of the lemma. For clearly each row of the same matrix differs in every place (column) since

$$\alpha^r(\beta + \delta) = \alpha^r(\gamma + \delta) \Rightarrow \beta = \gamma \qquad (\beta, \gamma, \delta \in GF(q)).$$

Just as obviously, each row of X differs from any row of $\alpha^r A$ in $q - 1$ places, since each element of $GF(q)$ appears exactly once in a row of $\alpha^r A$. Now suppose a row of $\alpha^r A$ agrees with a row of $\alpha^s A$ in two different places, where $\alpha^r \neq \alpha^s$. This means:

$$\alpha^r(\beta + \delta) = \alpha^s(\gamma + \delta) \qquad \text{and} \qquad \alpha^r(\beta + \varepsilon) = \alpha^s(\gamma + \varepsilon),$$
$$\text{where } \delta \neq \varepsilon.$$

Note that $\beta + \delta$ cannot $=0$, since this would imply that $\beta = \gamma$, which by the second equation implies $\alpha^r = \alpha^s$. Similarly, the other three sums cannot $=0$. But then:

$$\begin{aligned} \alpha^{r-s} &= (\gamma + \delta)(\beta + \delta)^{-1} = (\gamma + \varepsilon)(\beta + \varepsilon)^{-1} \\ &\Rightarrow (\gamma + \delta)(\beta + \varepsilon) = (\gamma + \varepsilon)(\beta + \delta) \\ &\Rightarrow \gamma\beta + \delta\beta + \gamma\varepsilon + \delta\varepsilon = \gamma\beta + \varepsilon\beta + \gamma\delta + \varepsilon\delta \\ &\Rightarrow \gamma(\varepsilon - \delta) = \beta(\varepsilon - \delta) \\ &\Rightarrow \gamma = \beta. \end{aligned}$$

But this implies $\alpha^r = \alpha^s$, a contradiction. So two rows of different matrices cannot agree in two places. Q.E.D.

DEFINITION. A Hadamard matrix H can be defined as an $n \times n$ matrix with entries from $\{1, -1\}$ so that $H \cdot H^T = nI$, where I is the identity matrix. This means that the real inner product between two different rows (when viewed as vectors in R^n) is 0. It is easy to show that except for $n = 1$ and $n = 2$, n must $\equiv 0 \pmod 4$. Hadamard matrices have several interesting properties, but the one we shall be concerned with is the following: If the -1's are replaced by 0's, an $n \times n$ binary matrix is obtained where the Hamming distance between any two rows is exactly $= n/2$.

If a Hadamard matrix has been given, then it is possible to construct new Hadamard matrices by permuting or complementing rows and columns. Hence a Hadamard matrix with all 1's in the first row and column can be obtained. This is known as a normalized Hadamard matrix.

Sylvester has shown that given an $n \times n$ Hadamard matrix we can always obtain a $2^k n \times 2^k n$ Hadamard matrix in the following fashion: Let $\bar{H}_n$ denote the matrix consisting of the complements of the rows of Hn. Then $H_{2n} = \left[\begin{smallmatrix} Hn & Hn \\ Hn & \bar{H}n \end{smallmatrix}\right]$ is also a Hadamard matrix. Proceed inductively for the general case.

Paley, by using quadratic residues, has shown that Hadamard matrices exist whenever $n = p + 1$, p a prime $\equiv 3 \pmod 4$. It is conjectured that Hadamard matrices exist $\forall n \equiv 0 \pmod 4$.

Notation. Throughout the rest of the paper let H_n denote a normalized $n \times n$ binary Hadamard matrix. For example,

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \qquad H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Let $\hat{H}_n$ denote H_n with the first column deleted. Let v_i denote the ith row of H_n, viewed as a vector in Z_2^n (define $\hat{v}_i$ similarly). Let $d(a, b)$ denote the Hamming distance between two vectors. Let $\bar{}$ denote complementation, whether of a vector or a matrix. Finally for C to be an (n, k, d) code means that $C \subset Z_2^n$, where $|C| =$ the number of vectors in $C = 2^k$ (so $k = \log_2 |C|$) and $d(a, b) \geqslant d$, $a, b \in C$.

Remark. If v_i, v_j come from H_n, $i \neq j$, then $d(v_i, v_j) = d(\bar{v}_i, v_j) = d(v_i, \bar{v}_j) = d(\bar{v}_i, \bar{v}_j) = n/2$. Note also that $d(\hat{v}_i, \hat{v}_j) = d(\bar{\hat{v}}_i, \bar{\hat{v}}_j) = n/2$ while $d(\hat{v}_i, \bar{\hat{v}}_j) = d(\bar{\hat{v}}, \hat{v}_j) = n/2 - 1$.

With the preliminaries out of the way, the basic method of construction,

lending itself to a fairly generalized description, may now be presented. Variations on the method, most of which require a more ad hoc treatment, will be listed afterwards. Specific examples and a table will follow.

Basic Construction. Look at $GF(2^k)$ (to avoid trivialities assume $k \geqslant 2$) and let $n \leqslant 2^k$. By the lemma, we can construct 2^k sets of 2^k vectors each in $GF(2^k)^n$, where the Hamming distance within a set $=n$, and the Hamming distance between sets $\geqslant n-1$. Now identify each element in $GF(2^k)$ with a distinct row of H_{2^k} (which by Sylvester's construction always exists) and insert that row wherever the element it is identified with occurs. The result is 2^{2k} binary vectors of length $n \cdot 2^k$ with minimum distance $=2^{k-1}(n-1)$. Call this set Q.

Observe that with respect to minimum distance between vectors in Q, it does not matter if $\bar{v}_i$ is used in place of v_i. That is, suppose we are given two distinct vectors x and y in Q, and we create two new vectors, x' and y', by complementing some of the Hadamard rows which make up x and y. Then, applying the first equality in the previous remark, we have the following:

$$d(x, y) = d(x', y) = d(x, y') = d(x', y').$$

Furthermore, the equality still holds whether or not the method for transforming x into x' was the same as that for transforming y into y'. Thus Q can be augmented via an appropriate complementing scheme.

So let C be a code from Z_2^n with minimum distance $=\lceil (n-1)/2 \rceil$ (least integer not less than) of maximal size. Then, given a vector x in Q, let $C(x)$ be the set of vectors in $Z_2^{n \cdot 2^k}$ constructed by using in turn each vector in C as a complementing scheme for x; i.e., applying each vector in C to x by complementing the Hadamard row in the jth block whenever a 1 occurs in the jth co-ordinate of the complementing vector. Since $d(v_i, \bar{v}_i) = 2^k$, it follows that if $a, b \in C(x)$, $d(a, b) \geqslant 2^k((n-1)/2) \geqslant 2^{k-1}(n-1)$; while if $x \neq y$ and $a \in C(x)$ and $b \in C(y)$, then the previous equality gives $d(a, b) = d(x, y) \geqslant 2^{k-1}(n-1)$. So the code: $\bigcup_{x \in Q} C(x)$ has length $n \cdot 2^k$, minimum distance $=2^{k-1}(n-1)$ and size $=|C| \cdot 2^{2k} = |C| \cdot |Q|$.

EXAMPLE. Construct the code over $GF(4)^4$ in the manner prescribed by the lemma, and transform it into a code in Z_2^{16} by making the following identification between elements of $GF(4)$ and rows of H_4:

$$0 \to 1111,$$

$$1 \to 1010,$$

$$\alpha \to 1100,$$

$$\alpha^2 \to 1001.$$

For instance, the vector $(0\ 1\ \alpha\ \alpha^2)$ becomes $(1111\ 1010\ 1100\ 1001) = x \in Z_2^{16}$. Now let C be the set of even weight vectors in Z_2^4. Then $C(x)$ (using the same x) is:

$C(x)$				C			
(1111	1010	1100	1001)	(0	0	0	0)
(1111	1010	0011	0110)	(0	0	1	1)
(1111	0101	1100	0110)	(0	1	0	1)
(1111	0101	0011	1001)	(0	1	1	0)
(0000	1010	0011	1001)	(1	0	1	0)
(0000	0101	1100	1001)	(1	1	0	0)
(0000	1010	1100	0110)	(1	0	0	1)
(0000	0101	0011	0110)	(1	1	1	1)

Then $\bigcup_{x \in Q} C(x)$ gives the code.

Let $A(n, d)$ represent the maximum number of codewords possible with length n and minimum distance d. A famous result of Plotkin's, known as the Plotkin Bound, gives an upper bound on $A(n, d)$ in three out of four cases. That is,

$$\text{when } n \equiv 0 \pmod 4 \; A(n, [(n-1)/2]) \leqslant 2n,$$

$$\text{when } n \equiv 2 \pmod 4 \; A(n, [(n-1)/2]) \leqslant n + 2,$$

$$\text{when } n \equiv 3 \pmod 4 \; A(n, [(n-1)/2]) \leqslant 2n + 2.$$

Furthermore, Levenshtein has shown that provided Hadamard matrices of certain orders exist (the largest of which would be $n+2$ for $n \equiv 2$ (4)) then the Plotkin Bound can actually be explicitly met. Also, $A(n, (n-1)/2) \geqslant 2n-2$ for $n \equiv 1$ (4) if a Hadamard matrix of size $n-1$ exists. Since Hadamard matrices are known to exist for all multiples of 4 up to 268, it follows that for $n \leqslant 266$, the three inequalities above are actually equalities, and we have a lower bound on $A(4a+1, 2a)$.

Now let $s(n)$ represent the largest number of *known* codewords of length n and minimum distance $=\lceil (n-1)/2 \rceil$. Then applying this complementary set to Q gives a $(2^k n,\ 2k + \log_2 s(n),\ 2^{k-1}(n-1))$ code. Let this be a code of type X with parameters n and k, written as $X(n, k)$. Deleting a co-ordinate gives $(2^k n - 1,\ 2k + \log_2 s(n),\ 2^{k-1}(n-1) - 1)$ code. Denote it by $Y(n, k)$. Finally, the lemma may be used. Identify each of the 2^k sets in Q with a distinct vector in Z_2^k, and tag that vector onto each vector of the set. Then apply the complementing set, ignoring the tag for the purposes of complementation. Since the distance within a set is $2^{k-1}n$, the minimum

distance is increased by 1, if n is even. If n is odd, it will be necessary to use a complementing set with minimum distance $=(n+1)/2$ in order to increase the overall distance of the code. If we let $t(n)$ represent the largest number of known code-words of length n and minimum distance $=\lceil (n+1)/2 \rceil$, then we have a $(2^k n + k,\ 2^k + \log_2 s(n),\ 2^{k-1}(n-1)+1)$ code for n even, and a $(2^k n + k,\ 2^k + \log_2 t(n),\ 2^{k-1}(n-1)+1)$ code for n odd. Denote it by $Z(n,k)$. Of course, using even weight vectors of length $k+1$ gives a $(2^k n + k + 1,\ 2^k + \log_2[s(n) \text{ or } t(n)],\ 2^{k-1}(n-1)+2)$ code. Denote it by $Z'(n,k)$.

The Plotkin Bound also gives an upper limit on $t(n)$: for every $n \equiv 1(2)$, $t(n) \leqslant (n+3)/2$. (We're only interested in the case n odd.) As before, Levenshtein's construction shows that for $n < 266$, the Plotkin Bound is tight (i.e., can be explicitly met).

The results of all this are summarized in the following porposition:

PROPOSITION 1. *Under the technique of associating rows of H_{2^k} with elements of $GF(2^k)$ after partitioning a subset $GF(2^k)^n$ in the manner prescribed by the lemma, it is possible to construct explicitly via a complementing scheme, codes with the following parameters*:

$$\vdots$$

$$(2^k n,\ 2k + \log_2 s(n),\ 2^{k-1}(n-1)) - \text{type } X,$$

$$(2^k n - 1,\ 2k + \log_2 s(n),\ 2^{k-1}(n-1) - 1) - \text{type } Y,$$

$$\left.\begin{array}{l}(2^k n + k,\ 2k + \log_2 s(n),\ 2^{k-1}(n-1)+1)n \equiv 0(2)\\ (2^k n + k,\ 2k + \log_2 t(n),\ 2^{k-1}(n-1)+1)n \equiv 1(2)\end{array}\right\} - \text{type } Z,$$

$$\left.\begin{array}{l}(2^k n + k,\ 2k + \log_2 s(n),\ 2^{k-1}(n-1)+1)n \equiv 0(2)\\ (2^k n + k,\ 2k + \log_2 t(n),\ 2^{k-1}(n-1)+1)n \equiv 1(2)\end{array}\right\} - \text{type } Z'$$

$$\vdots$$

Furthermore, for $n \leqslant 266$, we can always substitute for $\log_2 s(n)$:

$$\log_2 2n \text{ when } n \equiv 0(4),$$

$$\log_2(2n-2) \text{ when } n \equiv 1(4),$$

$$\log_2(n+2) \text{ when } n \equiv 2(4),$$

$$\log_2(n+2) \text{ when } n \equiv 3(4),$$

noting that except for the case $n \equiv 1(4)$, the numbers given are an absolute maximum for $\log_2 s(n)$. Similarly, when $n < 266$ and n is odd, we can replace $\log_2 t(n)$ with $\log_2(n+3)/2$ with this number being an absolute maximum for $\log_2 t(n)$.

Remark. For any practical purpose, the restriction that $n \leqslant 266$ is not much of a restriction. Since n must also $\leqslant 2^k$, we would have to be talking about a code of length $> 266 \cdot 512 = 136,\ 192$ before the Plotkin Bound could not be *automatically* assumed to be met.

Variations. Several variations are possible, often requiring a treatment peculiar to the particular parameters involved. These are listed below:

(i) When $n \equiv 1(4)$, it may be that $s(n) > 2n - 2$ (e.g., when $n = 5$, $(n-1)/2 = 2$ so $s(n) = 2^4$). So this should be ckecked.

(ii) Rows from $\hat{H}_{2^k}$ instead of H_{2^k} may be used. Since $d(\hat{v}_i, \bar{\hat{v}}_j) = 2n - 1$, minimum distance will be lost when the complementing set is applied. Hence the exact nature of the complementing set must be investigated (see Proposition 3 for an example).

(iii) Shorter tags may be attached to fewer sets when the type Z code is constructed.

(iv) For $k \geqslant 3$, longer tags may be added in order to increase the minimum distance by 3 or more.

(v) A distinct Hadamard row may be tagged onto each set, so that a complementing set from Z_2^{n+1} may be applied.

(vi) Apply the lemma twice (or more). That is, identify each element within a set with an element of $GF(q)$, and then arrange them according to the statement of the lemma. This will allow the use of a complementing set of dimension up to q^2. Of course, tags of various sorts may be attached.

EXAMPLE. The first two examples are the most important, since they better known results, and are therefore stated as propositions.

PROPOSITION 2. *Using the techniques described above, it is possible to explicitly construct a* $(51, 9, 21)$ *code.*

Proof. $Z(6, 3)$ does the trick. Since $n \equiv 2 \pmod 4$, this is really a corollary to Proposition 1. Q.E.D.

Previously, 2^8 was the largest number of codewords of length 51 and minimum distance 21. These were obtained via Zinoviev's Construction.

PROPOSITION 3. *Using the techniques described above, it is possible to explicitly construct a* $(52, 10, 21)$ *code.*

Proof. This makes use of variation (ii). Let $n = 7$, use rows from $\hat{H}_8$, and let $C = \{\hat{H}_8 \cup \bar{\hat{H}}_8\}$ be the complementing set. In this manner 2^{10} vectors in Z_2^{49} are created. Since the distance between any two vectors in C is 3, 4, or 7; and since $(\hat{v}_i, \hat{v}_j) = 4$ while $(\hat{v}_i, \bar{\hat{v}}_j) = 3$ when $\hat{v}_i$, $\hat{v}_j$ are rows of $\hat{H}_8$, it

follows that the minimum distance between the codewords in Z_2^{49} is $4 \cdot 2 + 3 \cdot 4 = 20$, and the distance between codewords in the same set (as categorized in the lemma) is at least 21. Hence the addition of a tag from Z_2^3 to each set creates a (52, 10, 21) code. Q.E.D.

COROLLARY. *There exists an alternate construction of a* (51, 9, 21) *code.*

Proof. Applying tags from Z_2^2 to half of the sets (as constructed in Proposition 3) yields a (51, 9, 21) code.

Previously, 2^9 was the largest number of codewords of length 52 and minimum distance 21. Again, these were constructed via Zinoviev's construction.

The following examples give parameters where this construction equals the best known results, as listed in Sloane and MacWilliams' table. A brief description of the method used is also given.

(i) (17, 6, 7)—Start off in $X(4, 2)$ and use variation (iii), i.e., tag on a 0 or a 1 to two of the sets.

(ii) (18, 7, 7)—This is $Z(4, 2)$.

(iii) (19, 8, 7)—Start out with $X(4, 2)$ and use variation (v), i.e., add a row from H_4 as the tag and use even weight vectors from Z_2^5 as the complementing set. Finally, delete a co-ordinate.

(iv) (27, 9, 9)—This is another application of variation (ii). With the exception that rows from $\hat{H}_8$ instead of H_8 are used, construct $X(4, 3)$. If even weight vectors from Z_2^4 are used as the complementing set, a (28, 9, 10) code is obtained. Deleting a co-ordinate yields the listed parameters.

(v) (31, 6, 15)—Take *one* set from $X(4, 3)$ and delete a co-ordinate.

(vi) (32, 6, 16)—Same as (v), only don't delete a co-ordinate.

(vii) (35, 9, 13)—This is $Z(4, 3)$.

(viii) (38, 9, 15)—This is an application of variation (iv). Start out with $X(4, 3)$ and use vectors from the (6, 3, 3) Hamming code as the tags.

(ix) (39, 10, 15)—This is $Y(5, 3)$ with variation (i) taken into account. If even weight vectors from Z_2^5 are used as the complementing set, the complementing set has size 2^4 instead of 2^3.

(x) (40, 10, 16)—This is $X(5, 3)$, with the same observation as in (ix).

(xi) (43, 8, 17)—This is $Z(5, 3)$, save that the (5, 2, 3) Hamming code is used as the complementing set.

(xii) (46, 8, 19)—This is the same as (xi), save that vectors from the (6, 3, 3) Hamming code are used as the tags.

(xiii) (46, 10, 17)—Look at the code constructed in Proposition 3. Instead of adding tags to the sets, delete three co-ordinates.

(xiv) (47, 9, 19)—This is $Y(6, 3)$.

(xv) (48, 10, 19)—This is the same as in (xiii), save that only one co-ordinate is deleted.

(xvi) (49, 10, 20)—This is the same as (xv), save that no co-ordinates are deleted.

(xvii) (50, 8, 21)—This uses variation (iv). Tags from Z_2^2 are attached to four of the sets in $X(6, 3)$ (see the corollary to Proposition 3).

(xviii) (51, 12, 17)—This uses variation (vi). Look at $X(3, 2)$ before complementing. Then for each set, arrange the vectors in the manner prescribed by the lemma, with $n = 4$. If a row from H_4 is attached to denote which set is being used, we have 2^6 vectors in Z_2^{52}, with 13 blocks of rows from H_4. Applying a (13, 6, 5) code as the complementing set and then deleting a co-ordinate gives the stated parameters.

(xix) (53, 10, 21)—This is obtained by deleting three co-ordinates from $X(7, 3)$.

(xx) (53, 8, 23)—Attach tags from the (5. 2. 3) Hamming code to four of the sets in $X(6, 3)$.

(xxi) (54, 9, 23)—Attach tags from the (6, 3, 3) Hamming code to each set in $X(6, 3)$ (see (xix)).

(xxii) (55, 10, 23)—This is $Y(7, 3)$.

(xxiii) (56, 10, 24)—This is $X(7, 3)$.

(xxiv) (65, 10, 29)—This is $Z(8, 3)$.

It is certainly possible that more results might be obtained by the techniques described in this paper. It is also possible that other variations might be useful.

ACKNOWLEDGMENTS

I would like to thank Professor Edwin Weiss of Boston University for his encouragement and advice. I would also like to thank F. J. MacWilliams and N. J. A. Sloane for writing their invaluable reference work, "The Theory of Error-Correcting Codes."

RECEIVED: September 22, 1979; REVISED: December 20, 1979

APPENDIX

Parameters for Which This Construction Is Best: (2)

(51, 9, 21) betters Zinoviev's (51, 8, 21)

(52, 10, 21) betters Zinoviev's (52, 9, 21)

Parameters for Which This Construction Equals Best Known Results: (24)

(17, 6, 7) equals Golay
(18, 7, 7) equals Golay
(19, 8, 7) equals Golay
(27, 9, 9) equals Piret
(32, 6, 16) equals Reed–Muller
(31, 6, 15) equals Reed–Muller
(35, 9, 13) equals *X* constructon applied to *BCN* code
(38, 9, 15) equals Goppa Code
(39, 10, 15) equals Goppa Code
(40, 10, 16) equals *X* construction applied to a cyclic code
(43, 8, 17) equals Goppa Code
(46, 8, 19) equals Helgert–Stenoff construction
(46, 10, 17) equals Hashara extended *BCH* codes
(47, 9, 19) equals Helgert–Stinoff
(48, 10, 19) equals Helgert–Stinoff
(49, 10, 20) equals Linear Code
(50, 8, 21) equals Goppa Code
(51, 12, 17) equals Karlin Linear Code
(53, 10, 21) equals Zinoviev
(53, 8, 23) equals Zinoviev
(54, 9, 23) equals Zinoviev
(55, 10, 23) equals Zinoviev
(56, 10, 24) equals Delsarte–Goethols generalized Kerdock Code
(6, 7, 10, 29) equals construction *X*

REFERENCES

LEVENSHTEIN, V. I. (1981), The application of Hadamard matrices to a problem in coding, *Problemy Kibernet.* **5**, 123–136. English translation in *Problems of Cybernetics* **5** (1964), 166–184 [2, A].

MACWILLIAMS, F. J. AND SLOANE, N. J. A. (1977), "The Theory of Error Correcting Codes" North-Holland, Amsterdam.

PLOTKIN, M. (1960), Binary codes with specified minimum distances, *IEEE Trans. Inform. Theory* **6**, 445–450.